What is claimed is:

1. A cryptographic communication method in which a communication key is used for enciphering data to be transmitted in the transmission side, and a key is used for decoding received data in the reception side, wherein in the transmission side an individual key that is different from the communication key is used for enciphering the data to be transmitted, the enciphered data are decoded by using the individual key first, and then the decoded data are enciphered by using the communication key so that the enciphered file can be transmitted.

2. The cryptographic communication method according to claim 1, wherein a file identifier of the original data is embedded in a file name, and a new identifier indicating that the data are the enciphered data are added to the data when enciphering the data by using the communication key.

3. A cryptographic communication method in which a key is used for enciphering data to be transmitted in the transmission side, and a communication key is used for decoding received data in the reception side, wherein in the reception side the received data are decoded by using the communication key, and then the decoded data are enciphered to be memorized by using an individual key that is different from the communication key, and the decoded data are erased.

4. The cryptographic communication method according to claim 1, wherein an authentication is performed independently for the individual key and the communication key so that the enciphering or the decoding can be performed by using the individual key and the communication key.

5. The cryptographic communication method according to claim 3, wherein an authentication is performed independently for the individual key and the communication key so that the enciphering or the decoding can be performed by using the individual key and the communication key.

6. A cryptographic communication method in which a communication key is used for enciphering data to be transmitted in the transmission side, and a communication key is used for decoding received data in the reception side, wherein an identification code corresponding to the communication key used for the enciphering is added to the enciphered data when enciphering in the transmission side, and in the reception side the communication key corresponding to the identification code is used for the decoding.

7. The cryptographic communication method according to claim 6, wherein plural communication keys are prepared in the transmission side, one of the keys is used for enciphering data, and an identification code corresponding to the key used for the enciphering is added to the enciphered data.

8. The cryptographic communication method according to claim 6, wherein plural communication keys are prepared in the reception side, and one of the communication keys that corresponds to the identification code is selected to be used.

9. A file access system, wherein two different keys are authenticated individually so that they can be used, and a decoding process using one of the keys and an enciphering process using the other of the keys are performed continuously for one file.

10. A file access system, wherein two different keys are authenticated individually so that they can be used, it is decided

whether a target file is enciphered, the target file is decoded by using one of the keys if the target file is enciphered, the target file is not processed if the target file is not enciphered, and the other of the keys is used for enciphering the unenciphered file.

11. A file access system, wherein two different keys are authenticated individually so that they can be used, an enciphered file is decoded by using one of the keys, it is decided whether a target folder for storing the file is for encipher files, the file is enciphered by using the other of the keys and is stored if the target folder is for encipher files, and the file is stored without any process if the target folder is for encipher files.

12. A file access system, wherein a display including a first folder and a second folder is performed, decoding and/or enciphering process of a file stored in the first folder when an instruction is inputted for moving the file from the first folder to the second folder, and the decoded and/or enciphered file is stored in the second folder.

13. The file access system according to claim 12, wherein it is decided whether the file stored in the first folder is enciphered, the file is decoded by using a first key if the file is enciphered, the file is not processed if the file is not enciphered, and then the unenciphered file is enciphered by using a second key.

14. A computer-readable recording medium on which a program of file access is recorded, the program being for a computer to perform the process comprising the steps of:

authenticating two different keys individually so that they can be used; and

performing a decoding process by using one of the keys and an enciphering process by using the other of the keys

continuously for one file.

15. An encipher processing device that is used for a cryptographic communication in which a communication key is used for enciphering data to be transmitted in the transmission side, and a key is used for decoding received data in the reception side, the device comprising:

the communication key;

an individual key that is different from the communication key; and

a process portion for performing a decoding process by using the individual key and an enciphering process by using the communication key continuously.